ABSTRACT:

An access system with original, authorized access keys (2) is described, wherein the access system and the original access keys (2) comprise pseudo-random generators supplying an identical, secret cryptographic key, an identical cryptographic algorithm and identical numerical sequences, which are usable for mutual authentication in a challenge-response method. For the purpose of learning one or more additional, non-original access keys (4) comprising a pseudo-random generator supplying equal numerical sequences,

- an authentication is performed at the access system (1) with an original access key (2),
- the access system (1) and an additional access key (4) to be learnt are set to a learning mode,
- the access key (4) to be learnt transmits its individual identifier identifying the access key (4) to the access system (1),
- the access system (1) transmits the secret cryptographic key encrypted by means of a number supplied by its pseudo-random generator to the access key (4) to be learnt, which decrypts and stores this key by means of the same number supplied by its pseudo-random generator, and
- the access system (1) stores the identifier of the learnt access key (4) and performs a mutual authentication with the learnt access key (4) which is subsequently usable as an access key.

Figure